IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Proudler, Graeme John	Examiner:	Moran, Randal
Serial No.	10/688,397	Art Unit:	2135
Filed:	10/16/2003	Our Ref:	621375 200309650
For:	"Method and Apparatus for Managing a Hierarchy of Nodes"	Date:	June 30, 2008
		Re:	*Reply Brief*

REPLY BRIEF

Mail Stop Appeal Brief - Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Sir:

This is a Reply Brief filed pursuant to 37 CFR 41.41 in an Appeal taken from the Final Rejection, dated September 5, 2007, for the above identified patent application. A Notice of Appeal was filed on December 4, 2007 and an Appeal Brief was filed on February 4, 2008. The Examiner's Answer is dated April 30, 2008. Appellants submit that this Reply Brief is being timely filed on June 30, 2008.

The Examiner did not number the pages in his Answer. When referring to the Answer below the Applicant has numbered the pages of the Answer with the page bearing the title "BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES" as page 1 thereof.

The Decrypted Access Arrangement

On page 7 of the Answer the Examiner asserts that "Applicant agrees that Challenger discloses 'the decrypted access arrangement'". **This assertion is incorrect.**

Claim 35 calls for, *inter alia*:

> "a decrypted-access arrangement arranged to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key;" [Emphasis added]

The Appeal Brief argues at page 6, second paragraph:

> "The Examiner argues at the top of page 3 of the Final Official Action that Challener teaches "the decrypted-access arrangement" (but not the current-decryption-root setting arrangement). However, Challener does not have any arrangement for restricting "decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key". This is because the only "current decryption-root key" disclosed in Challener is the storage root key itself and all the hierarchy nodes are decryptable by a chain of decryption rooted in the storage root key – therefore there is no concept of less than the whole hierarchy being decryptable in Challener and therefore no concept of an arrangement restricting decrypted access to a subset of the nodes of the hierarchy."

The very limitation which the Examiner asserts that the Applicant admits is present in Challener, is the same limitation which the Applicant very clearly demonstrates is absent in Challener in the paragraph repeated above.

The Examiner then quotes a passage from Challener on pages 7-8 of the Answer and opines on what Challener teaches on page 8. In the first line following the quote from Challener the Examiner says:

> "Challener explicitly discloses a decrypted access arrangement (i.e. the storage root key being used to decrypt all leaf nodes below it)."

As the Applicant has explained in the passage from the Appeal Brief quoted above, the "decrypted access arrangement" of claim 35 explicitly does not permit decryption of all leaf nodes below the storage root key – the decrypted access arrangement restricts (i.e. limits) decrypted access to those nodes decryptable by a chain of decryption rooted in the current decryption-root key.

On page 9 of the Answer, at lines 10-11 of the Examiner commentary, the Examiner again asserts that"

> "Applicant agrees that Challener discloses 'the decrypted access arrangement' (Appeal Brief- p.6, para 2)"

This is not correct.

Although the Applicant has agreed that Ishiguro discloses a "current-decryption root setting arrangement" the Appilcant also points out (Appeal Brief, page 9, para 4) that:

> "An important point to note is that: Ishiguru has no concept of an arrangement for restricting access to only some of the hierarchy nodes because Ishiguru always starts with the available key that is highest up the hierarchy. Nodes of the hierarchy that are higher up than this starting key are de facto inaccessible without any need to provide an arrangement to restrict access."

The Applicant strongly disagrees with the Examiner's assertion at the bottom of page of the Answer:

> "Therefore, the combination of Challener and Ishiguro explicitly discloses a decrypted-access arrangement to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key."

No such restriction is occurring.

The Rationale for Combining Challener and Ishiguro

The Examiner states on page 10 of his Answer that the rationale for combining the 'decrypted access arrangement' of Challener (which is not, in fact, present) with the 'decryption-root setting arrangement' of Ishiguro is:

> "to provide a decoding apparatus in which encryption keys can be managed with ease."

This is a mere conclusory statement which clearly ignores the teachings of the cited art to the contrary. In Ishiguro the Examiner-stated goal of managing encryption keys with ease is achieved by employing a linear hierarchy of keys that are all related to one another so that one starting key provides access to all keys lower in the hierarchy thereby facilitating key management. As noted in the Appeal Brief (page 11, lines 16-18), the required security properties of the Challener TPM (trusted platform module) make it highly undesirable that the keys of its key hierarchy are cryptographically related to each other. Therefore the solution of Ishiguro is contradictory to the teaching of Challener and would be positively avoided by anyone wishing to improve on Challener. The Examiner's rationale is not only merely conclusory, it is totally inadequate. The Examiner concocts this rationale for combining Challener and Ishiguro based on a hindsight reconstruction of Applicant's claims as opposed to that which the prior art really teaches and suggests to a person of ordinary skill in the art. The Examiner's stated rationale for combining Challener and Ishiguro does not pass muster under *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1734 (2007) cited in the Appeal Brief.

Conclusion

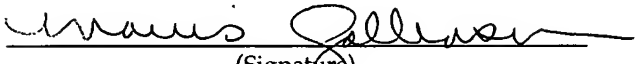
For the extensive reasons advanced in the Appeal Brief and for the reasons noted above, Appellants respectfully contend that each claim is patentable over the cited art. Therefore, reversal of all rejections is courteously solicited.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this Appeal Brief is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

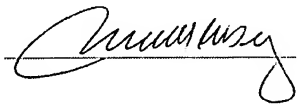
30 June 2008
(Date of Transmission)

Mavis Gallenson
(Name of Person Transmitting)


(Signature)

30 June 2008
(Date)

Respectfully submitted,



Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile